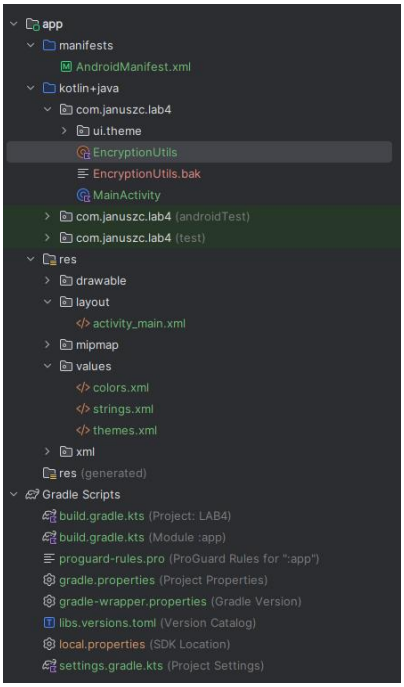
Laboratorium 4

Na ocenę 3.0:

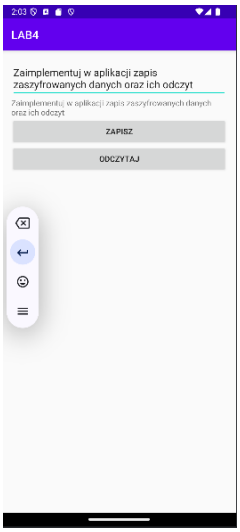
1. twórz nową lub użyj istniejącej aplikacji w Android Studio.

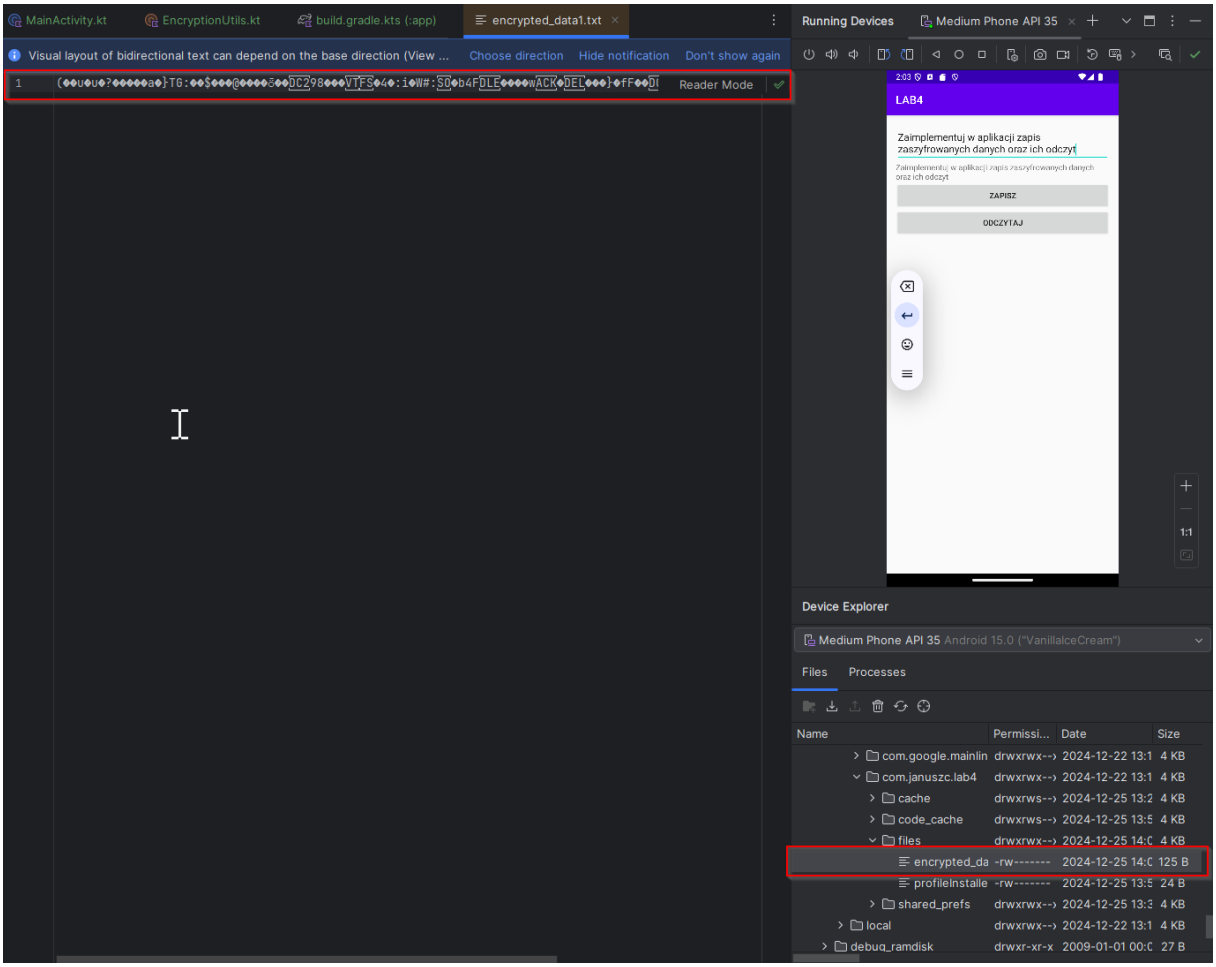


2. Dodaj bibliotekę security-crypto do dependencies w gradle

```
dependencies {

    implementation(libs.androidx.core.ktx)
    implementation(libs.androidx.lifecycle.runtime.ktx)
    implementation(libs.androidx.activity.compose)
    implementation(platform(libs.androidx.compose.bom))
    implementation(libs.androidx.ui)
    implementation(libs.androidx.ui.graphics)
    implementation(libs.androidx.ui.tooling.preview)
    implementation(libs.androidx.material3)
    //security crypto
    implementation(libs.androidx.security.crypto)
    implementation(libs.androidx.appcompat)
    implementation(libs.androidx.material)

    testImplementation(libs.junit)
    androidTestImplementation(libs.androidx.junit)
    androidTestImplementation(libs.androidx.espresso.core)
    androidTestImplementation(platform(libs.androidx.compose.bom))
    androidTestImplementation(libs.androidx.ui.test.junit4)
    debugImplementation(libs.androidx.ui.tooling)
    debugImplementation(libs.androidx.ui.test.manifest)
}
```

3. Zaimplementuj w aplikacji zapis zaszyfrowanych danych oraz ich odczyt





Plik został utworzony na urządzeniu, zapisane informacje są takie same. Próba bezpośredniego odczytu pliku pokazana na zrzucie ekranu. Brak możliwości odczytu oryginalnej wiadomości.

4. Implementacja w kodzie

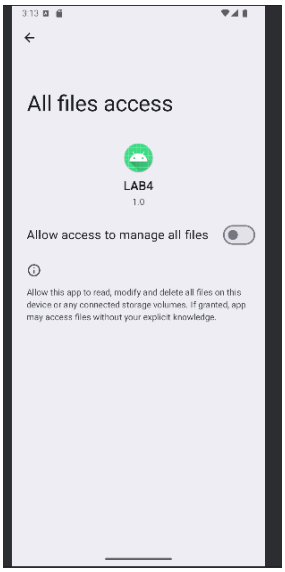
```
object EncryptionUtils_na3_0 {

    private const val FILE_NAME = "encrypted_data1.txt"

    fun saveEncryptedData(context: Context, data: String) {
        try {
            val masterKey = MasterKey.Builder(context)
                .setKeyScheme(MasterKey.KeyScheme.AES256_GCM)
                .build()

            val file = File(context.filesDir, FILE_NAME)
            val encryptedFile = EncryptedFile.Builder(
                context,
                file,
                masterKey,
                EncryptedFile.FileEncryptionScheme.AES256_GCM_HKDF_4KB
            ).build()

            encryptedFile.openFileOutput().use { outputStream ->
                outputStream.write(data.toByteArray(StandardCharsets.UTF_8))
            }

        } catch (e: Exception) {
            e.printStackTrace()
        }
    }
```

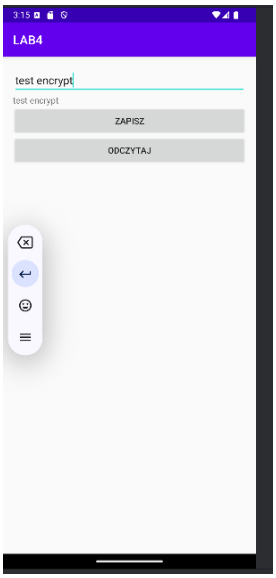
```
    fun loadEncryptedData(context: Context): String {
        return try {
            val masterKey = MasterKey.Builder(context)
                .setKeyScheme(MasterKey.KeyScheme.AES256_GCM)
                .build()

            val file = File(context.filesDir, FILE_NAME)
            val encryptedFile = EncryptedFile.Builder(
                context,
                file,
                masterKey,
                EncryptedFile.FileEncryptionScheme.AES256_GCM_HKDF_4KB
            ).build()

            encryptedFile.openFileInput().use { inputStream ->
                inputStream.readBytes().toString(StandardCharsets.UTF_8)
            }
        } catch (e: Exception) {
            e.printStackTrace()
            "Error loading data"
        }
    }
}
```

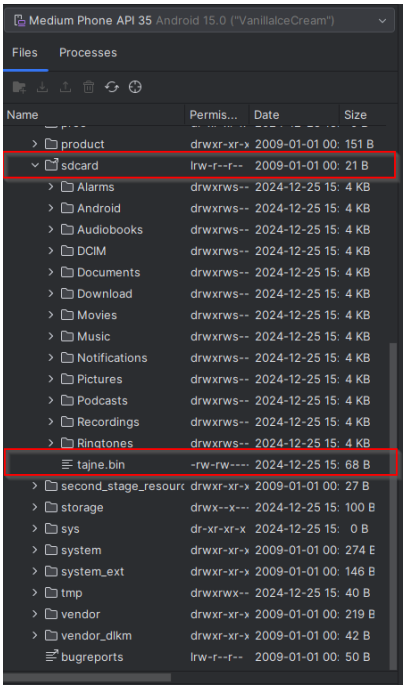
Plik dołączony do źródeł (EncryptionUtils_na3_0)

Na ocenę 3.5

1. Zrobić zapis pliku tajne.bin w pamięci wspólnej (/sdcard/) urządzenia


All files access
LAB4
1.0
Allow access to manage all files
Allow this app to read, modify and delete all files on this device or any connected storage volumes. If granted, app may access files without your explicit knowledge.


LAB4
test encrypt
test encrypt
ZAPISZ
ODCZYTAJ


Medium Phone API 35 Android 15.0 ("VanillaIceCream")
Files
Processes
Name
Permis...
Date
Size
product drwxr-xr-x 2009-01-01 00: 151 B
sdcard lrw-r--r-- 2009-01-01 00: 21 B
Alarms drwxrws--- 2024-12-25 15: 4 KB
Android drwxrws--- 2024-12-25 15: 4 KB
Audiobooks drwxrws--- 2024-12-25 15: 4 KB
DCIM drwxrws--- 2024-12-25 15: 4 KB
Documents drwxrws--- 2024-12-25 15: 4 KB
Download drwxrws--- 2024-12-25 15: 4 KB
Movies drwxrws--- 2024-12-25 15: 4 KB
Music drwxrws--- 2024-12-25 15: 4 KB
Notifications drwxrws--- 2024-12-25 15: 4 KB
Pictures drwxrws--- 2024-12-25 15: 4 KB
Podcasts drwxrws--- 2024-12-25 15: 4 KB
Recordings drwxrws--- 2024-12-25 15: 4 KB
Ringtones drwxrws--- 2024-12-25 15: 4 KB
tajne.bin -rw-rw---- 2024-12-25 15: 68 B
second_stage_resourc drwxr-xr-x 2009-01-01 00: 27 B
storage drwx--x--- 2024-12-25 15: 100 B
sys dr-xr-xr-x 2024-12-25 15: 0 B
system drwxr-xr-x 2009-01-01 00: 274 B
system_ext drwxr-xr-x 2009-01-01 00: 146 B
tmp drwxrwx--- 2024-12-25 15: 40 B
vendor drwxr-xr-x 2009-01-01 00: 219 B
vendor_dlkm drwxr-xr-x 2009-01-01 00: 42 B
bugreports lrw-r--r-- 2009-01-01 00: 50 B